



CYBER CENTER OF EXCELLENCE:

STRENGTHENING CRITICAL INFRASTRUCTURE

October 27, 2014

Statement A: Approved for public release, distribution is unlimited (27 OCTOBER 2014)



Agenda

1300 Pat Sullivan, Executive Director, SPAWAR

Overview

1330 Greg Hansford, SPAWAR Budget Officer, SPAWAR

CYBER Budget Outlook: Federal to SPAWAR

1400 Brian Marsh, Office of SPAWAR Chief Engineer

CYBER Security & Technical Authority

1430 Steve Bullard, Program Manager PMW 130

Information Assurance & Cyber Security

1500 CAPT Ben McNeal, Program Manager PMW 160

Afloat Tactical Networks Cyber Security

1530 CAPT Michael Abreu, Program Manager PMW 205

Ashore Naval Enterprise Networks Cyber Security

1600 Dr. Stephen Russell, Director, Science and Technology, SPAWAR

Cyber Security Science & Technology



Space and Naval Warfare Systems Command

"The U.S. Navy's Information Dominance Systems Command"

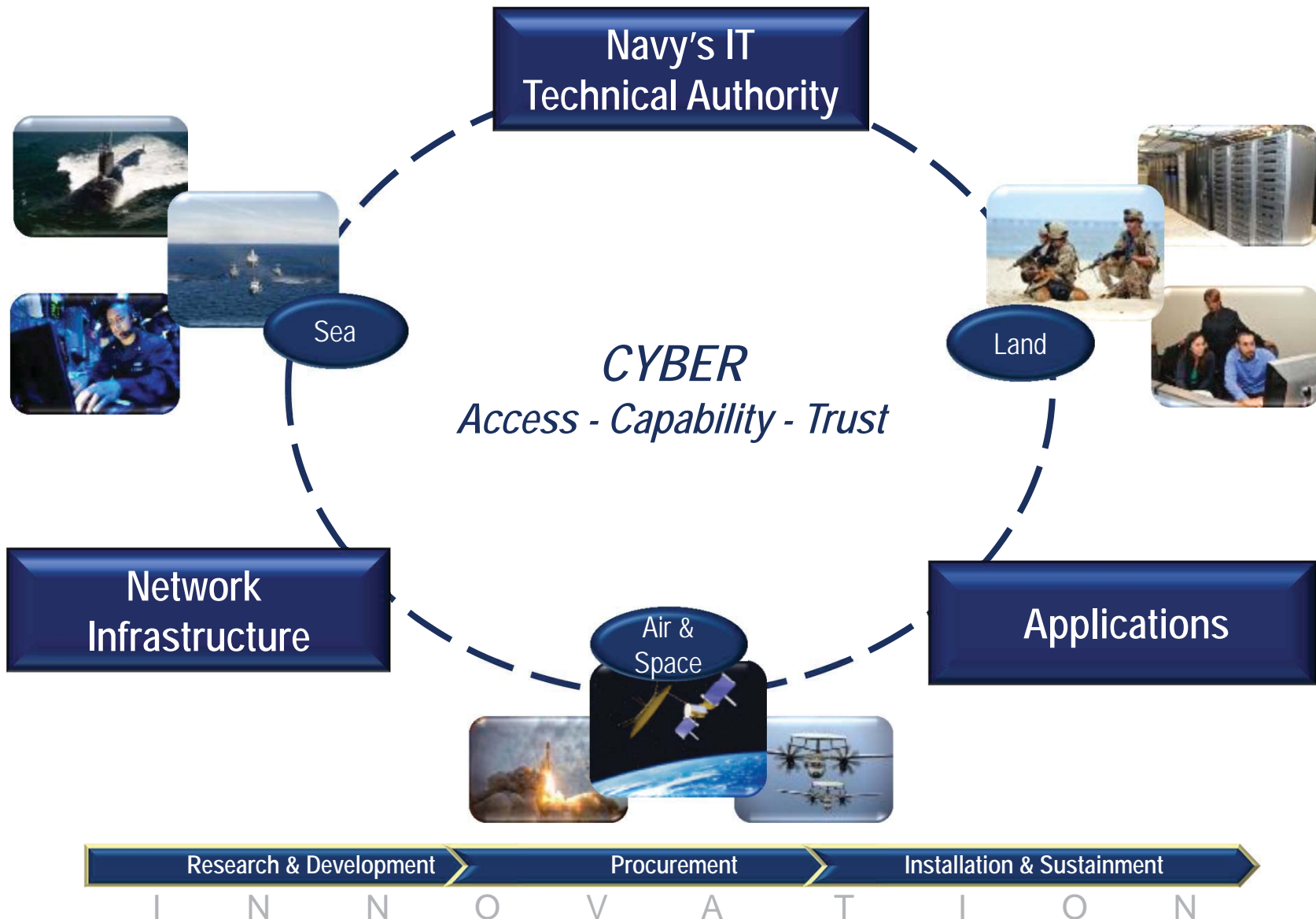
October 27, 2014

Presented to:
San Diego
Cyber Center of Excellence

Pat Sullivan
Executive Director

Statement A: Approved for public release, distribution is unlimited (27 OCTOBER 2014)

Supporting U.S. Navy Information Dominance





DoD Budget and the Cyber Response

27 October 2014

Presented to:
Cyber Center of Excellence:
Strengthening Critical
Infrastructure
Sheraton Mission Valley

Mr. Greg Hansford
Budget Officer,
Space and Naval Warfare
Systems Command

Statement A: Approved for public release, distribution is unlimited (21 OCTOBER 2014)



FY 2015 President's Budget Request

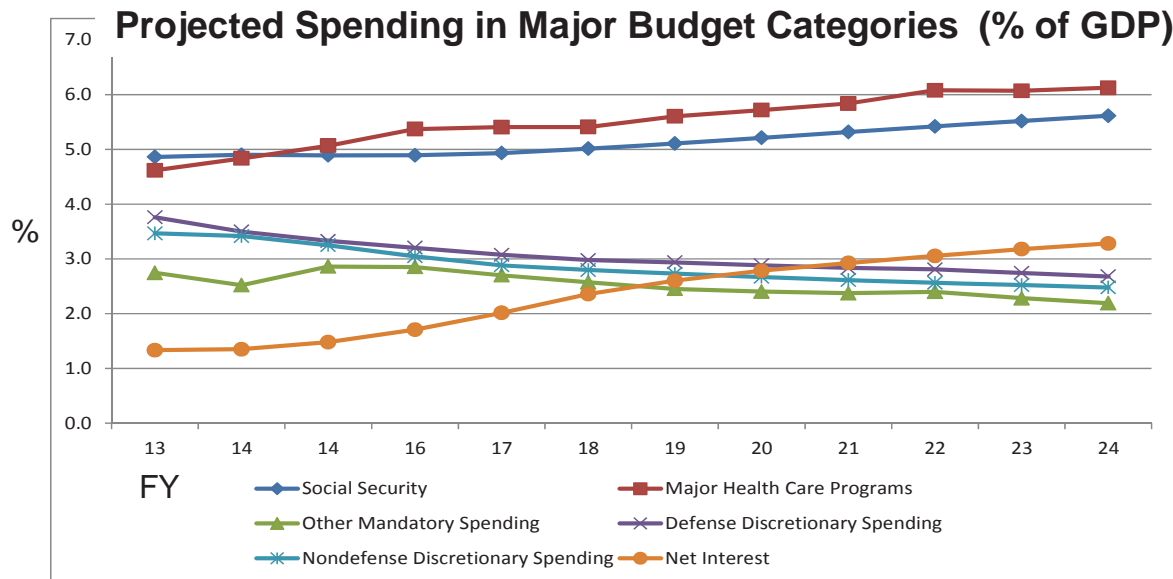
- ▼ Department of Defense = \$496B
- ▼ Department of the Navy = \$148B (29.8%)
- ▼ SPAWAR = \$3.8B (2.6% of Navy)
 - RDT&E,N = \$0.4B
 - OPN/WPN = \$1.7B
 - O&M,N = \$1.7B

RDT&E,N = Research, Development, Test and Evaluation, Navy

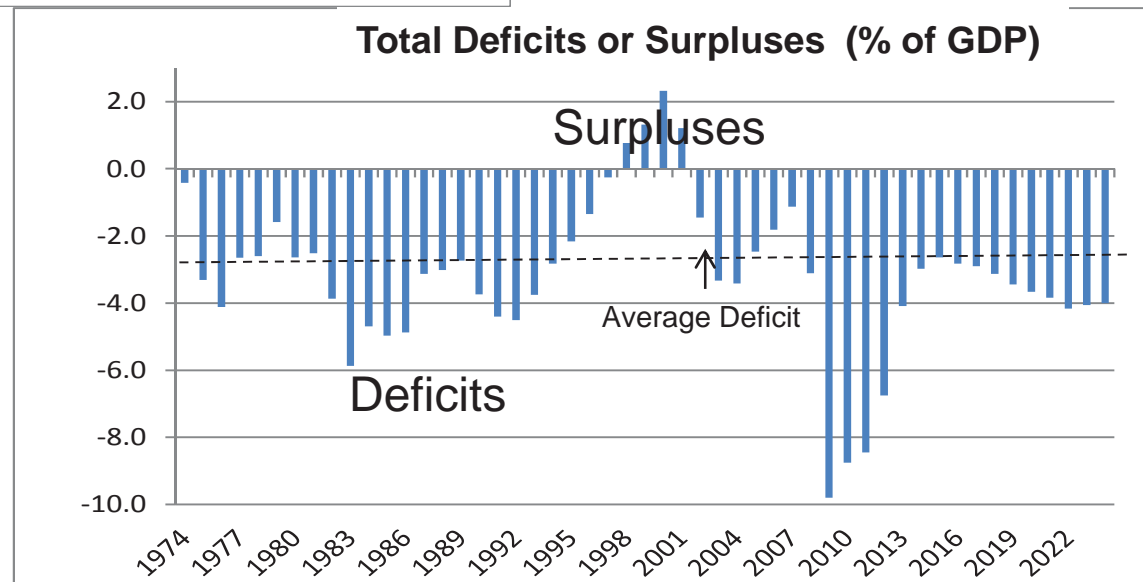
OPN/WPN = Other Procurement, Navy / Weapons Procurement, Navy

O&M,N = Operations & Maintenance, Navy

U.S. Fiscal Pressures



Deficits, interest payments, and entitlement spending are resulting in downward pressure to defense budgets



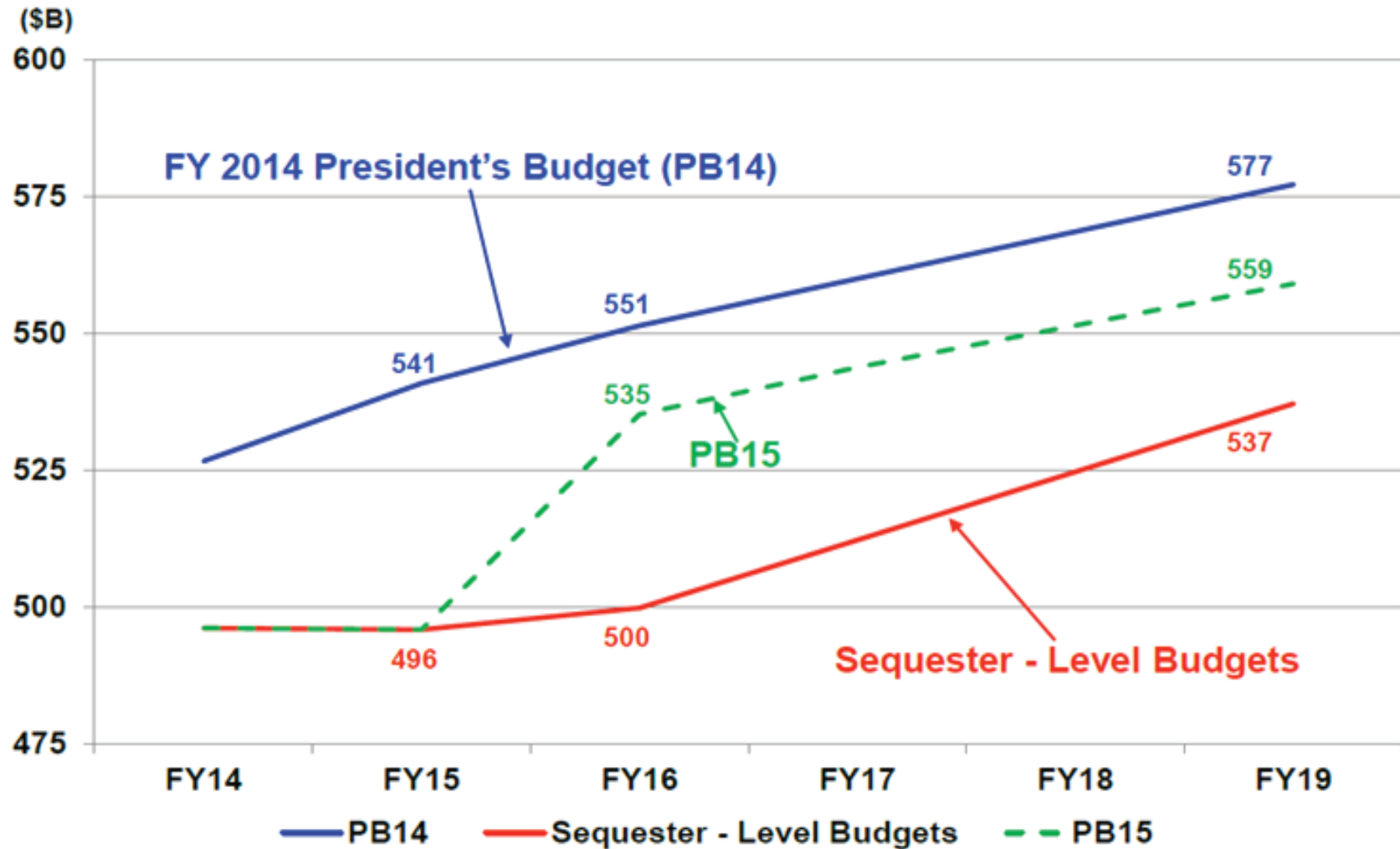


Today's Fiscal Environment

- **Budget Control Act (Aug 2011)**
 - Established 10-year discretionary budget caps (FY11 – FY21)
 - Reduced Defense budget ~\$487 billion over 10 years
 - Established committee to recommend additional \$1.5T in savings
 - Reduction incorporated in PB13: Navy -\$9.5B (FY13), -\$58.1B (FYDP)
- **Sequestration**
 - Failure of committee resulted in additional automatic reductions to Defense of ~\$600B over 10 years to begin Jan 2013
- **Bipartisan Budget Agreement (Dec 2013)**
 - Revised discretionary budget caps for FY14 and FY15 only
 - Reduced FY14 Defense sequester from -\$51.4B to -\$30.0B
 - Reduced FY14 Navy sequester from -\$15.4B to -\$9.4B



DoD PB15 Base-Budget Topline





What happened during the FY 2013 Sequestration to funds flow/execution?

- ▼ The short version is that everything slowed down significantly
- ▼ SPAWAR's FY 2013 budget was reduced by more than \$300M (a pro-rated 7.5% reduction)
- ▼ Deferred many Cyber / Information Assurance efforts
- ▼ Deferred some equipment procurements, increasing use of legacy equipment
- ▼ Deferred some design and development R&D efforts



What happens under a Continuing Resolution (CR) in terms of funds flow/execution?

- ▼ The President signs the CR (sometimes at the last minute)
- ▼ The CR funds Defense for a specific number of days
 - Funding for only that many days is provided to the Navy
 - CR's biggest funding impact is for R&D and procurement (OPN, etc.) as we only are funded for the CR number of days vice for the entire year
- ▼ Under a CR, we cannot start new efforts nor increase procurements to a higher rate than was funded in the previous year



Continuing Resolutions (CR)

-- A Historical Perspective --

FY	# CRs	CR #1 (# days & dates)	CR #2 (# days & dates)	CR #3 (# days & dates)	CR #4 (# days & dates)	CR #5 (# days & dates)	CR #6 (# days & dates)	CR #7 (# days & dates)	Total # days
FY 2003	3	4 10/1 – 10/4	7 10/5 – 10/11	7 10/12 – 10/18					18
FY 2004	0	N/A							0
FY 2005	0	N/A							0
FY 2006	3	50 10/1 – 11/19	29 11/20 – 12/18	12 12/19 – 12/30					91
FY 2007	0	N/A							0
FY 2008	1	43 10/1 – 11/12							43
FY 2009	0	N/A							0
FY 2010	3	31 10/1 – 10/31	48 11/1 – 12/18	5 12/19 – 12/23					84
FY 2011	7	64 10/1 – 12/3	15 12/4 – 12/18	3 12/19 – 12/21	73 12/22 – 3/4	14 3/5 – 3/18	21 3/19 – 4/8	7 4/9 – 4/15	197
FY 2012	5	4 10/1 – 10/4	45 10/5 – 11/18	28 11/19 – 12/16	1 12/17	6 12/18 – 12/23			84
FY 2013	1	178 10/2 – 3/27							178
FY 2014	2	107 10/1 – 1/15	3 1/16 – 1/18						110
FY 2015	1	72 10/1- 12/11							72

CRs have been the “norm” for the past six years.



Cyber Budgeting

- ▼ The Cyber threat continues to grow, and the slow Federal budget process is not well equipped to quickly respond
- ▼ Some funds for Cyber efforts were placed into the FY 2015 President's Budget request, but not enough
 - SPAWAR currently plans to receive over \$500M between now and FY 2020 to address the most critical requirements
- ▼ Development and review of the requirements is ongoing. Funding strategies will focus on the highest priority items.



Cybersecurity & Technical Authority



27 October 2014



Presented to:

Mr. Brian Marsh

Cyber Center of Excellence

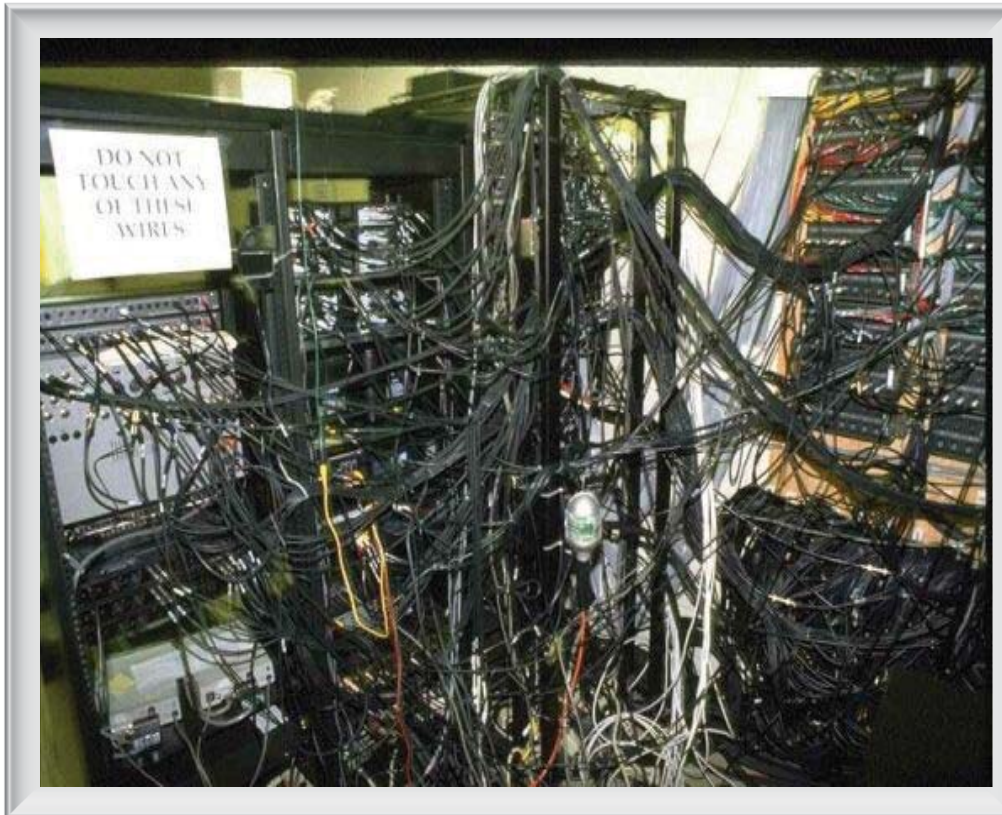
Assistant Chief Engineer
(Certification & Mission Assurance)
Space & Naval Warfare Systems Command

Statement A: Approved for public release, distribution is unlimited (21 OCTOBER 2014)



A System of Systems Engineering Challenge: Mitigating the Vulnerabilities

Our Enterprise Reality

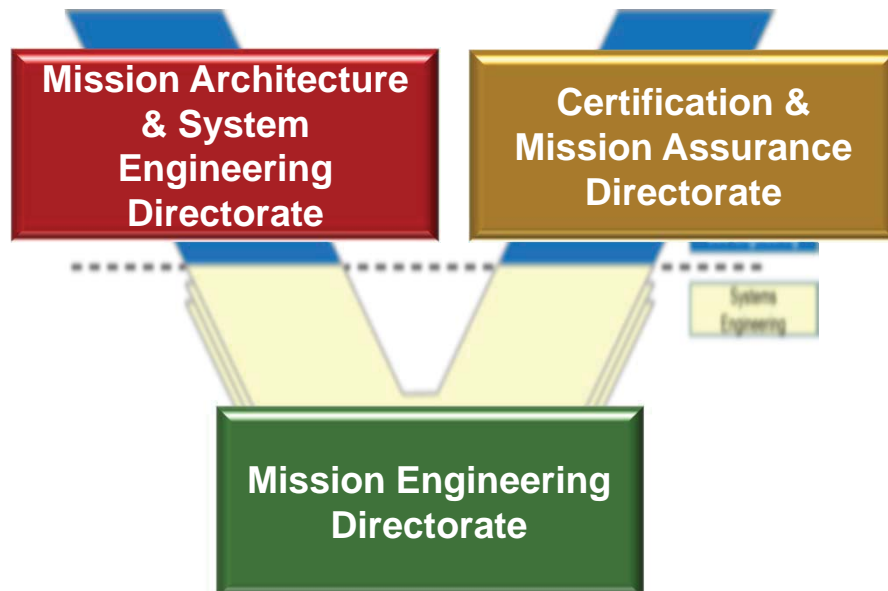


- ▼ A series of stovepipes wired together & not organized or aligned for effective interoperability
 - Little-to-no focus on System-of-Systems or Enterprise-level engineering
 - Integration & Interoperability an afterthought
- ▼ Resulting in an IT infrastructure that is:
 - Too large
 - Too old & too hard to upgrade
 - Too varied & expensive
 - Too hard to manage & operate
 - *Too hard to defend*

We Can't Live Like this Anymore in a Dirty & Contested Cyber World



Office of the Chief Engineer (CHENG) Roles & Responsibilities



Key Responsibilities:

- ▶ **Information Technology (IT) Technical Authority (TA)**
 - *Defining interface requirements & certifying compliance for Navy Systems to connect to the Navy IT Enterprise*
- ▶ **Information Assurance (IA) TA**
 - *Assuring the Warfighter's Cyber Dominance-- identifying & mitigating cyber security risks to the Navy IT Enterprise*
- ▶ **SYSCOM TA for PEO C4I, PEO EIS and PEO SPACE SYSTEMS**
 - *Providing specifications, standards, engineering processes to deliver / certify the programs*
- ▶ **Certification & Accreditation**
 - *Includes IA/Cyber Security Technical Authority (end-to-end)*
 - *Includes C4I certification - Interoperability, Integration, and IA*
- ▶ **National Competency Leadership**
 - *Command & Control (C2)*
 - *Intelligence, Surveillance & Reconnaissance (ISR) & Information Operations (IO)*
 - *Communications & Networks*



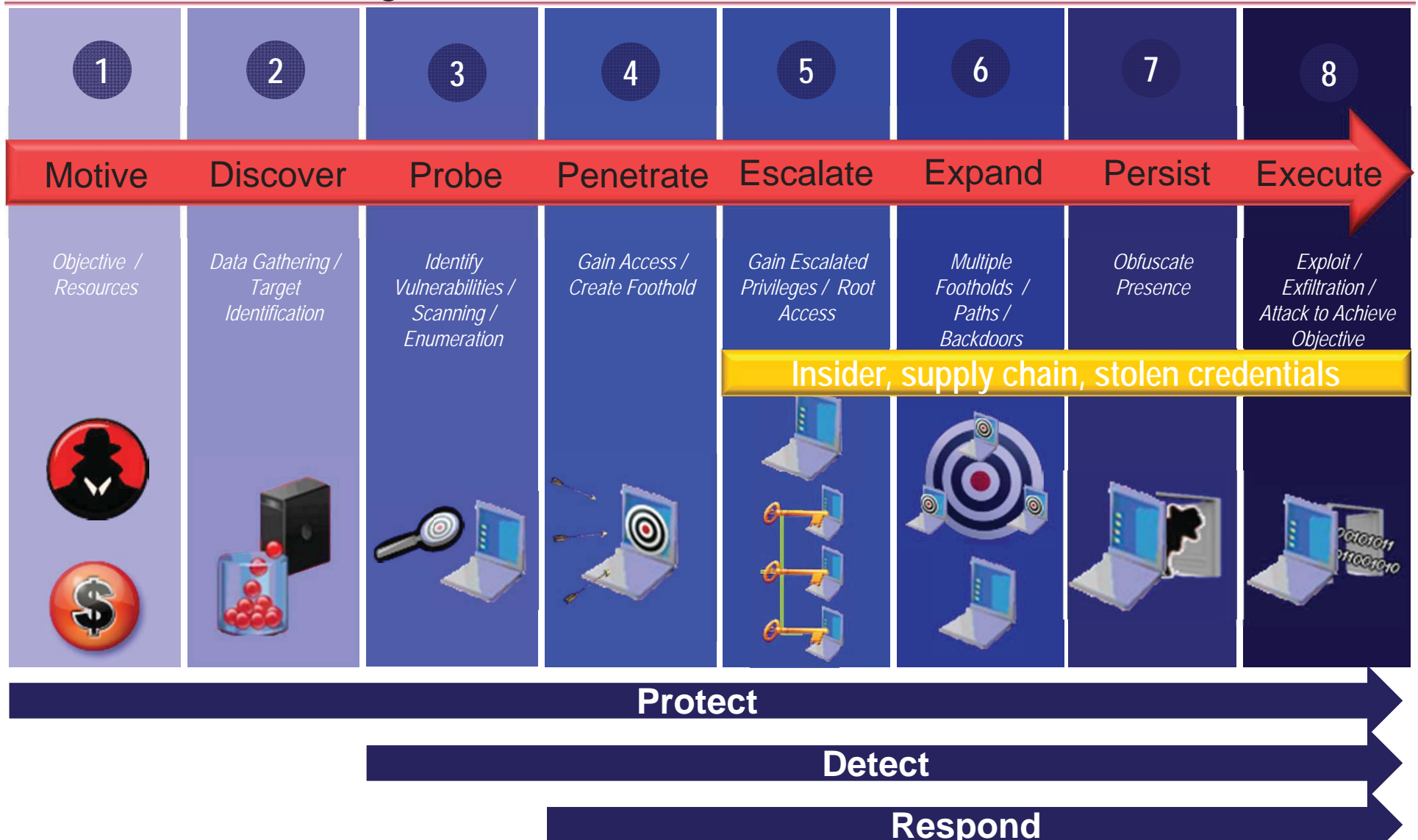
SPAWAR's Technical Authorities

SYSKOM Technical Authority	Information Assurance Technical Authority	Information Technology Technical Authority
Strong Systems Engineering Leadership	<i>Aligning the Navy's IT to an Enterprise Architecture</i>	
Common Processes and Practices	Converging to a Network with Inherited Security Controls	Converging to a Standard Computing Stack
Independent Voice on Technical Issues	Reducing Vulnerabilities by Balancing Risk with Operational Requirements	Reducing the Number of Unique Interfaces Internal and External to a Platform

Use SPAWAR's SYSKOM, IT & IA TA to Drive the Navy's Cyber Wholeness

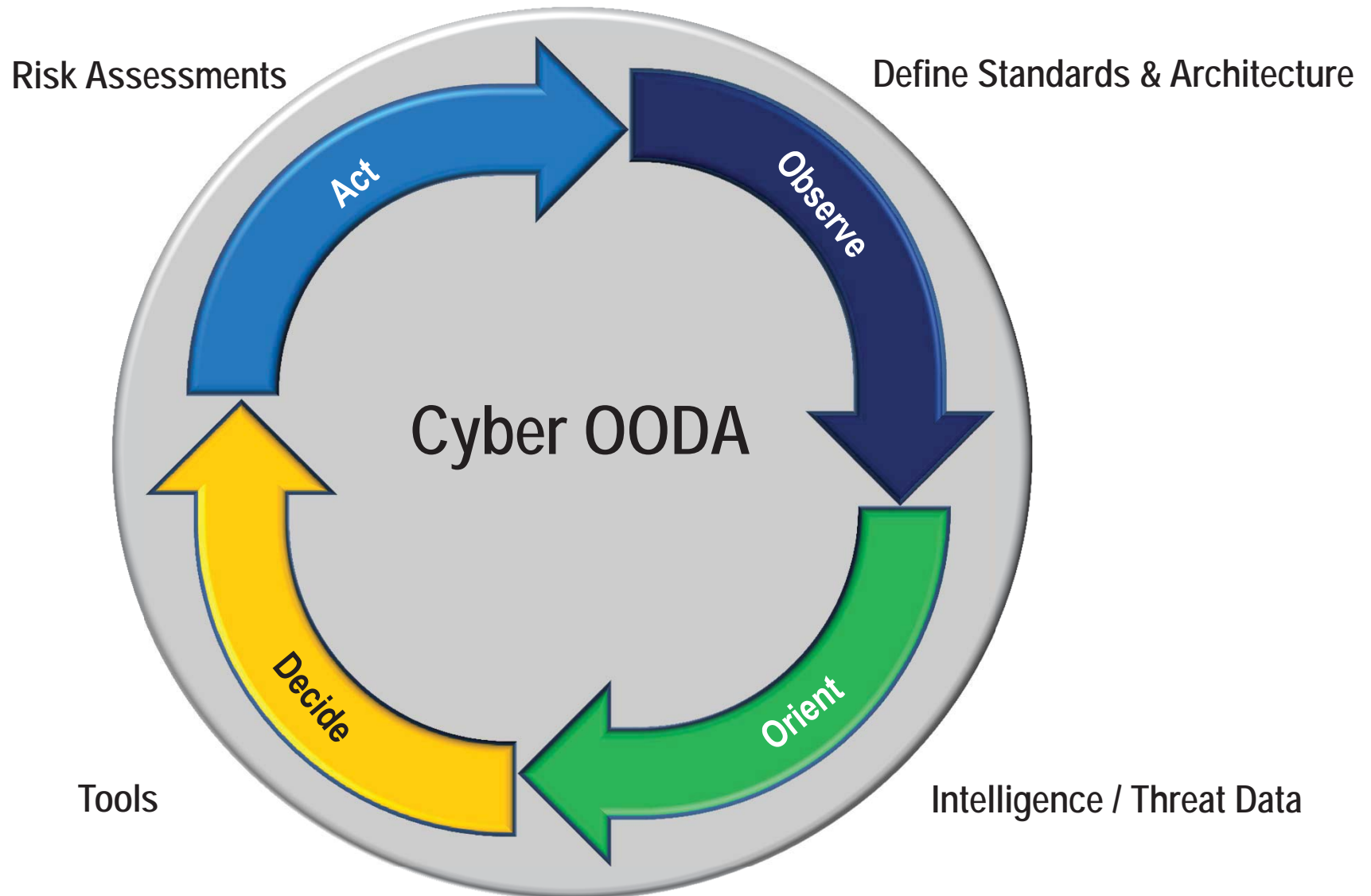


Understanding the Threat: Anatomy of an Attack





Cyber OODA Loop





Assessing the Vulnerabilities

SPAWAR 5.0 Cyber Risk Assessment Methodology

1

Scope platform, mission, and architecture

2

ID systems of interest across mission areas

3

Develop baseline modeling architecture

4

Develop specific risk / mitigation sets based on architecture (risk cubes)

5

Prioritize mitigations based on mission impact

Disciplined Engineering Approach to Understanding the Navy's Cyber Risk



Bad Cyber Impacts Navy

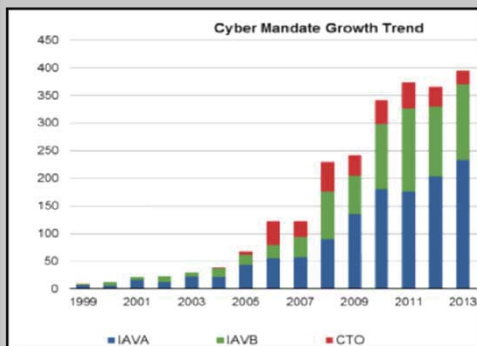
Information Assurance (IA) = Cybersecurity

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequence})$$

Dynamic & Growing



Exploitation Space

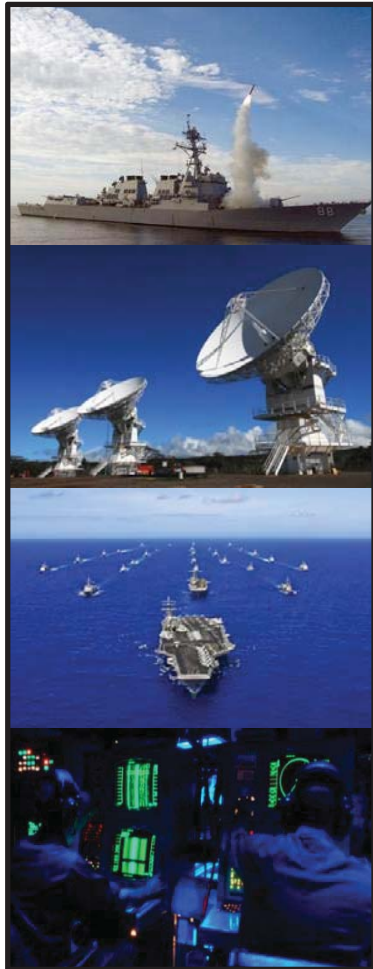


Impact to Mission





Effective Partnership with Industry is Vital to Improving Navy's Cyber Posture



What do we need from industry to help us?

1. Align programs/efforts with Standards & Processes
 - Standard products; no unique solutions
 - Open architectures & government purpose rights
 - Help define & tailor standards for specific warfighting missions
2. Minimize Variants
 - Minimize points of presence
 - Minimize the number of unique interfaces
3. Build for Cyber Agility
 - Adapt to changing threat
 - Latest thinking on cyber offense & defense-in-depth

President Barak Obama: "It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation"



**Program Executive Office
Command, Control, Communications,
Computers and Intelligence (PEO C4I)**

Cyber Center of Excellence (CCoE)
*Defending the Navy's Networks against the
Evolving Cyber Threat*

**27 October 2014
Mr. Steve Bullard
Program Manager (PMW 130)**

Statement A: Approved for public release; distribution is unlimited (21 OCTOBER 2014)

**Information Dominance
Anytime, Anywhere...**



PEOC4I.NAVY.MIL



PMW 130

What We Do



- Secure information, protect networks, and enable decision superiority throughout the cyber domain
- Navy Cryptography
 - Crypto Modernization (Crypto Products, Crypto Data, Crypto Voice)
 - Key Management (Electronic Key Management System (EKMS) and Key Management Infrastructure (KMI))
 - Public Key Infrastructure (PKI)
- Network Security
 - Computer Network Defense (CND)
 - Navy Cyber Situational Awareness (NCSA)
 - Navy's Cross Domain Solution (CDS) program of record



The Navy's Information Assurance and Cyber Security Program Office



Cryptography & Key Management Overview



- Acquire, install, and provide life cycle support for Type-1 end cryptographic units (ECU) for Navy, Marine Corps and Coast Guard platforms
- Programs include:
 - Cryptography (Data, Voice, Legacy)
 - EKMS / KMI / Key loader devices
 - PKI (NIPRNet and SIPRNet)





Computer Network Defense (CND) Overview



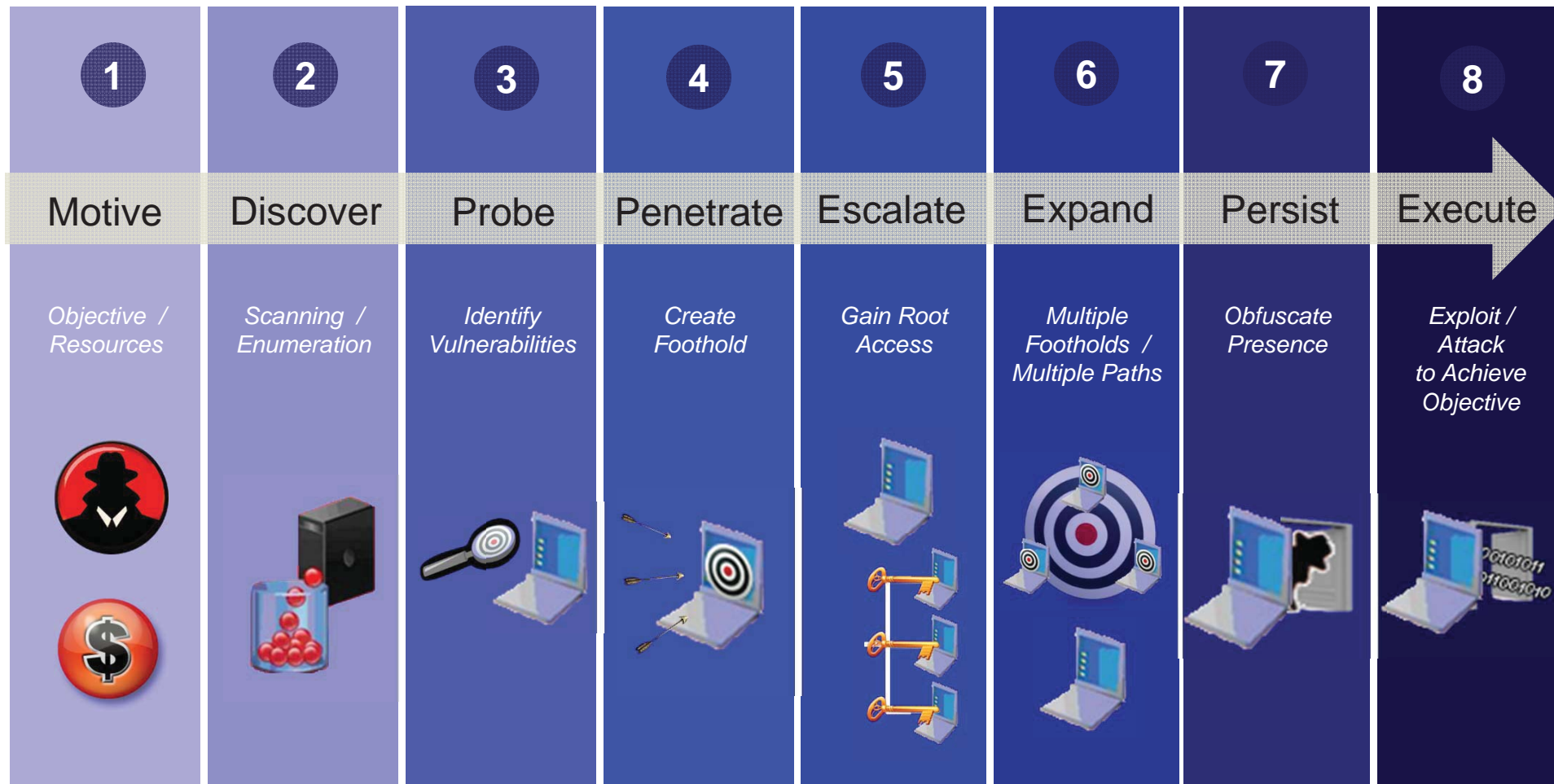
- Protects, monitors, analyzes, detects, and responds to unauthorized activity within Navy tactical networks and attacks against computer-network vulnerabilities, cyber threats, and critical assets
- Capabilities:
 - Shore: Firewalls, HBSS/HIPS, IDS/IPS, event logging, security compliance scanning and assessment, spyware/malware & anti-virus protection, email scanning gateway, VPNs, and web content filtering
 - Afloat: HBSS/HIPS, security compliance scanning and assessment

“Computer Network Defense (CND): Actions taken to protect [against], monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.”
-- DoDD O-8530.1, CND



Threat

Anatomy of an Attack





Motive

Money, Terrorism, Hacktivism, Espionage

1	2	3	4	5	6	7	8
Motive	Discover	Probe	Penetrate	Escalate	Expand	Persist	Execute
Objective / Resources	Scanning / Enumeration	Identify Vulnerabilities	Create Foothold	Gain Root Access	Multiple Footholds / Multiple Paths	Obfuscate Presence	Exploit / Attack to Achieve Objective

- In recent weeks, multiple, very large U.S. retailers have experienced significant data breaches
- Resulted in the theft of some 40 million payment card numbers and another 70 million customer records

<http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>



Discover

Catalog What's Out There



1	2	3	4	5	6	7	8
Motive	Discover	Probe	Penetrate	Escalate	Expand	Persist	Execute
Objective / Resources	Scanning / Enumeration	Identify Vulnerabilities	Create Foothold	Gain Root Access	Multiple Footholds / Multiple Paths	Obfuscate Presence	Exploit / Attack to Achieve Objective

- Exposed credit card and personal data: more than 110 million consumers
- Appears to have begun with a phishing attack sent to employees at an HVAC firm that did business with a nationwide retailer
 - HVAC company had external network access that was not cordoned off from its payment system network <http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>



Probe

Find Specific Weaknesses

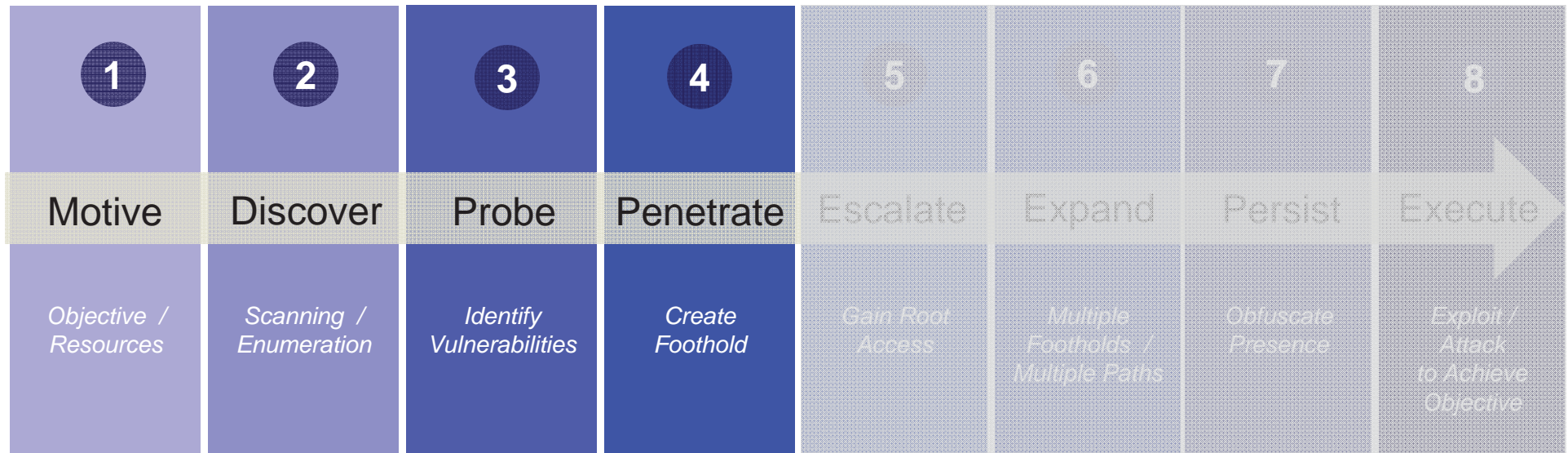
1	2	3	4	5	6	7	8
Motive	Discover	Probe	Penetrate	Escalate	Expand	Persist	Execute
Objective / Resources	Scanning / Enumeration	Identify Vulnerabilities	Create Foothold	Gain Root Access	Multiple Footholds / Multiple Paths	Obfuscate Presence	Exploit / Attack to Achieve Objective

- Malware, among other features, can "scrape" information from a compromised point-of-sale (PoS) terminal's memory while it's unencrypted

<http://www.eweek.com/security/target-breach-involved-two-stage-cyber-attack-security-reseachers.html#sthash.Xw7rbja7.dpuf>



Penetrate Gain Access



- Supply Chain: traced back to network credentials that were stolen from a third party refrigeration, heating, and air conditioning subcontractor

<http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>



Escalate

Increase Rights and Privileges

1	2	3	4	5	6	7	8
Motive	Discover	Probe	Penetrate	Escalate	Expand	Persist	Execute
Objective / Resources	Scanning / Enumeration	Identify Vulnerabilities	Create Foothold	Gain Root Access	Multiple Footholds / Multiple Paths	Obfuscate Presence	Exploit / Attack to Achieve Objective

- Two stage attack: penetrate via Industrial Control Systems to steal PoS data from a machine not connected to the Internet, then move that data to another machine which can in turn send it to an FTP (server)



Expand

Create New Points of Ingress/Egress

1	2	3	4	5	6	7	8
Motive	Discover	Probe	Penetrate	Escalate	Expand	Persist	Execute
Objective / Resources	Scanning / Enumeration	Identify Vulnerabilities	Create Foothold	Gain Root Access	Multiple Footholds / Multiple Paths	Obfuscate Presence	Exploit / Attack to Achieve Objective

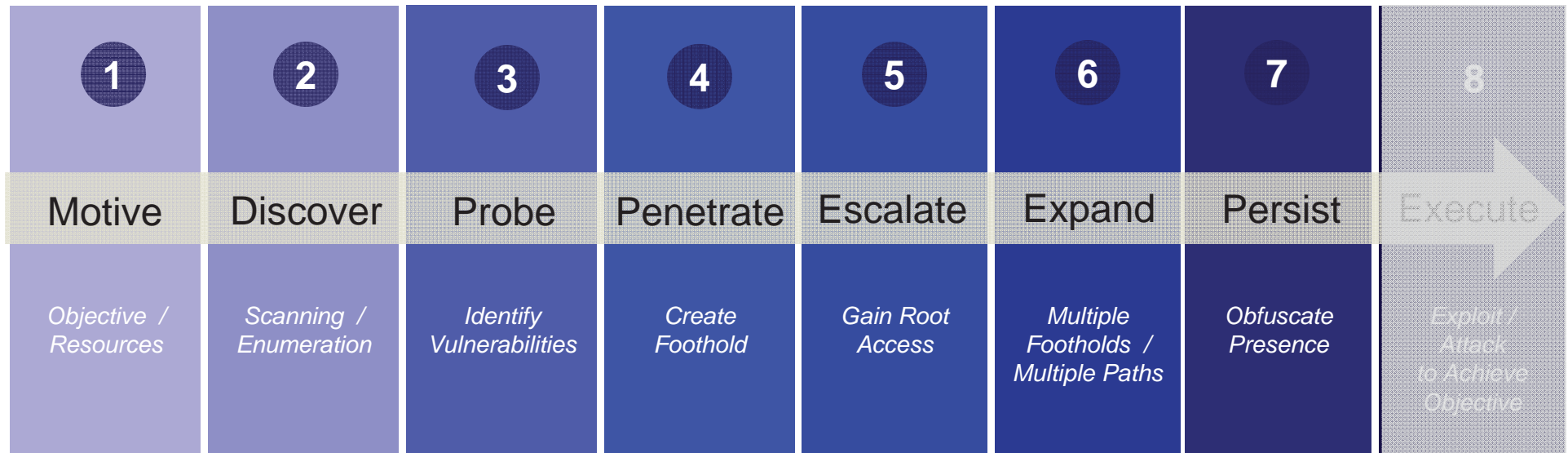
- Segregate Networks and Functions: found an Internet server that the attacker had used as a communications hub to retrieve information from a drop site within its own network

<http://www.eweek.com/security/target-breach-involved-two-stage-cyber-attack-security-reseachers.html#sthash.Xw7rbja7.dpuf>



Persist

Hide Until Ready to Execute



- Using a virtual private server in Russia, the attackers then downloaded the information
- The stolen data totaled 11GBs

<http://www.newsweek.com/target-meets-state-attorneys-lawsuits-pile-225085>



Execute *Achieve Objective*



- “Despite industry standards that require rapid application of security patches, some of these systems are updated inconsistently, especially in smaller retail environments without sophisticated IT organizations.”

<http://www.businessweek.com/articles/2014-01-14/worried-about-the-target-breach-add-this-term-to-your-vocabulary>

- Could be facing losses of up to \$420 million as a result of this breach
- Upgrading retailer’s systems to handle chip-and-PIN could cost \$100 million.

<http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>

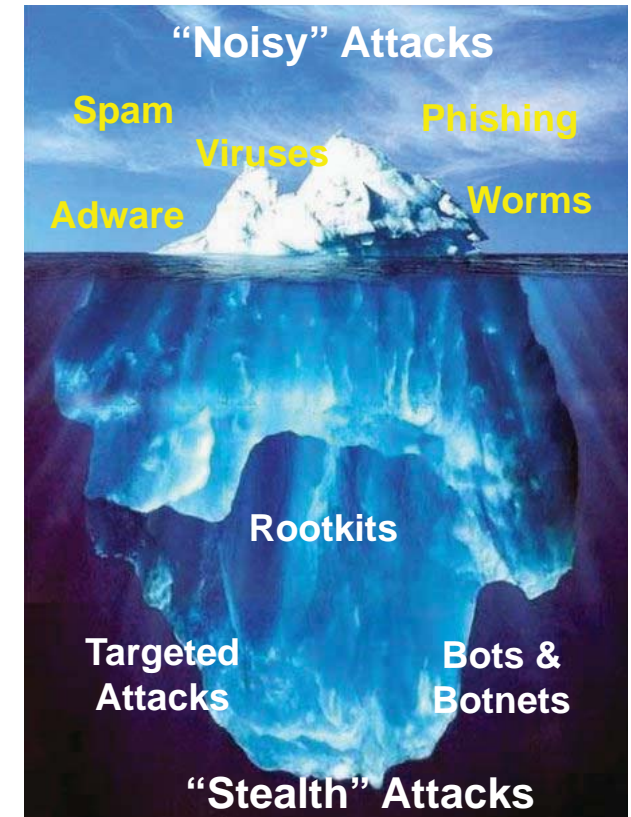


Navy Priorities

Focusing on the Cyber Threat



- Navy engineering, acquisition, fielding efforts are focused on:
 - More sensors in more places
 - Improved boundary protections
 - Proactive vice reactive capabilities
 - Better reporting, vulnerability scanning, and risk management strategies
 - Improved Cyber Situational Awareness
- Industry is needed to help us separate the noise from the important
 - Data analysis – proactive in the sense we are smarter about how we detect and separate data from multiple independent sensors
 - Link data to information to drive knowledge that leads to Decision Superiority





Cyber Defense and the Navy

What can Industry do for Us?

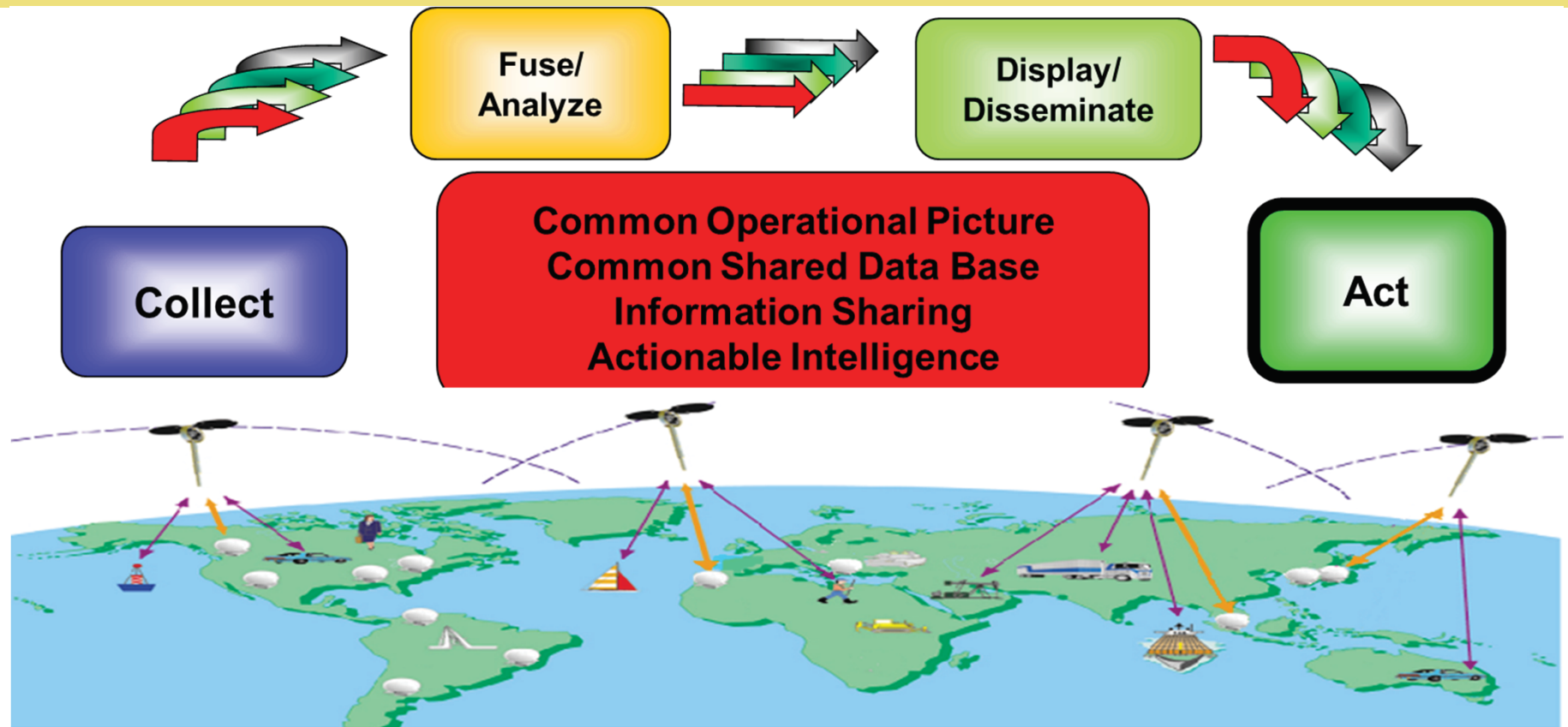


- Anomaly Detection
- Supply Chain
- Social Engineering
- Speed to Capability
- Industrial Control Systems
- Cyber SA / Continuous Monitoring
- Bring Your Own Device (BYOD)
- Education, Training, and Awareness
- Insider Threat





Cyber Situational Awareness / Continuous Monitoring



“We are building collective defenses with our allies. Just as our air defenses are linked to those of our allies to provide warning of aerial attack, so too can we cooperatively monitor our computer networks for cyber intrusions.”

William J. Lynn, III, Deputy Secretary of Defense
Remarks on Cyber at the RSA Conference
15 February 2011



PMW 130 Industry Partnerships



Contract Number	SPAWAR HQ Contract Title	Contractor (Prime)	Contract Type	Ceiling Amount	POP
N00178-05-D-4180 NS04	PMW 130/160 Installation Support	ANSOL	CPFF	\$4,825,652	10/1/2012 - 9/30/2017
N00178-14-D-8006 NS01	PMW 120/130 Financial Support Services	Artemis	CPFF	\$13,122,450	6/1/2014 - 5/31/2019
N00178-05-D-4611 NS06	PMW 160/130 Integrated Logistics Support	TCI	CPFF	\$4,151,539	10/1/2012 - 9/30/2017
N00178-04-D-4024 NS41	PMW 130 Information Assurance, PM & Tech Spt	Booz Allen	CPFF	\$65,763,728	10/1/2012 - 9/30/2017
N00039-14-D-0013	Radiant Mercury Sustainment	LMCO	CPFF	\$45,000,000	9/1/2014 - 8/31/2019
N00039-11-C-0039	LINK-22 Units	Raytheon	CPFF	\$12,129,321	3/1/2011 - 12/31/2014

Note: light blue rows indicate small business

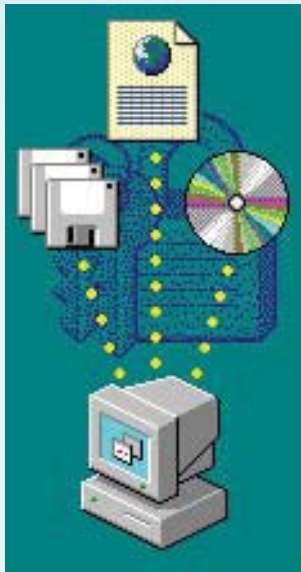
PMW 130 teamed with Industry to support the Navy and PEO C4I's Cybersecurity mission



The Way Ahead for Cybersecurity

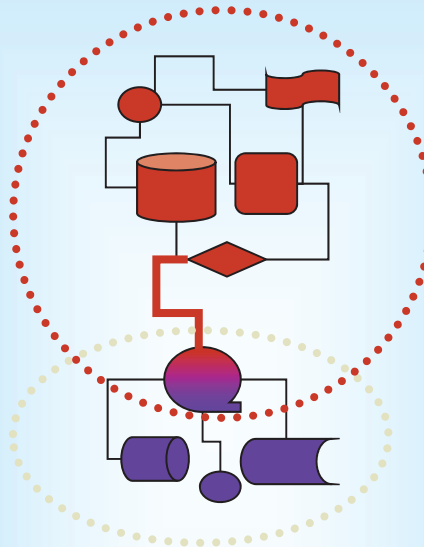


TODAY



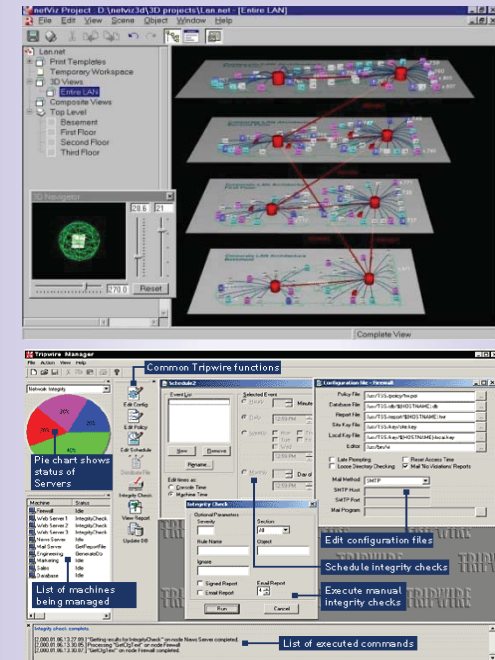
***Limited Interoperability
based on point solutions
that are built and fielded
independently***

INTERMEDIATE



***Field and integrate a
broader spectrum of netted
cybersecurity sensors to
provide Situational
Awareness and enable
Information Dominance***

TARGET



***Cybersecurity privileges
dynamically adjusted to
reflect the security
posture of the warfighter
and the DoDIN as a
whole***



**Program Executive Office
Command, Control, Communications,
Computers and Intelligence (PEO C4I)**

Afloat Tactical Networks Cybersecurity

**October 2014
CAPT Ben McNeal
Program Manager PMW 160
619.524.7909
ben.mcneal@navy.mil**

Distribution Statement A: Approved for public release, distribution is unlimited (21 OCTOBER 2014)

***Information Dominance
Anytime, Anywhere...***



PEOC4I.NAVY.MIL



Today's Afloat Tactical Networks



- **Consolidated Afloat Networks and Enterprise Services (CANES)**
 - Local Area Network (LAN) functionality for ships and submarines
 - Installations completed on ten destroyers and one aircraft carrier
 - Fourteen installations ongoing on three aircraft carriers, one large deck amphibious ship, one smaller amphibious ship, two cruisers and seven destroyers
- **Automated Digital Network System (ADNS)**
 - Wide Area Network (WAN) for Navy IP network operations
 - Distributes data between various shipboard networks and available Radio Frequency (RF) paths including satellite communications
 - Secure, rapid, reliable information exchanges for voice, video, and data



Aircraft Carrier



Destroyer



Maritime Operations Center



Landing Ship



Cruiser



Virginia Class



Amphibious Assault Landing Platform Dock





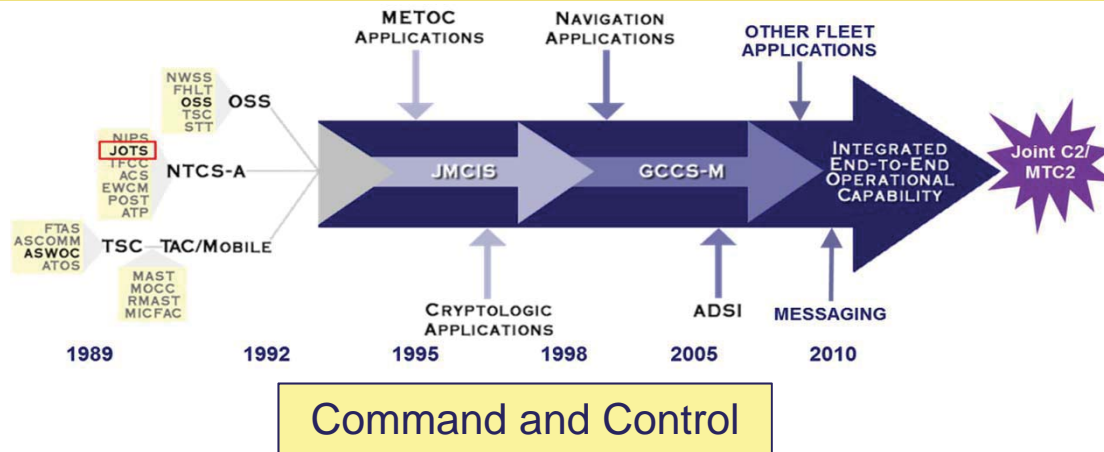
Background

How We Got Here

- **Evolution of Navy Afloat Tactical Networks**
 - Networks initially designed and installed for single function
 - Logistics, command and control, personnel management, etc.
- **Implications for Cybersecurity**
 - Significant variance with numerous hardware and software instantiations
 - Weak Configuration Management
 - Multiple variations to secure
 - Significant end of life and end of support challenges
- **Challenges**
 - Modernization and maintenance timelines
 - Form, Fit, Function Replacements
 - Cybersecurity tools
 - Cybersecurity training
 - Threat prediction and recognition
 - Supply Chain Risk Management - COTS



Command and Control and Supply / Logistic System Evolution



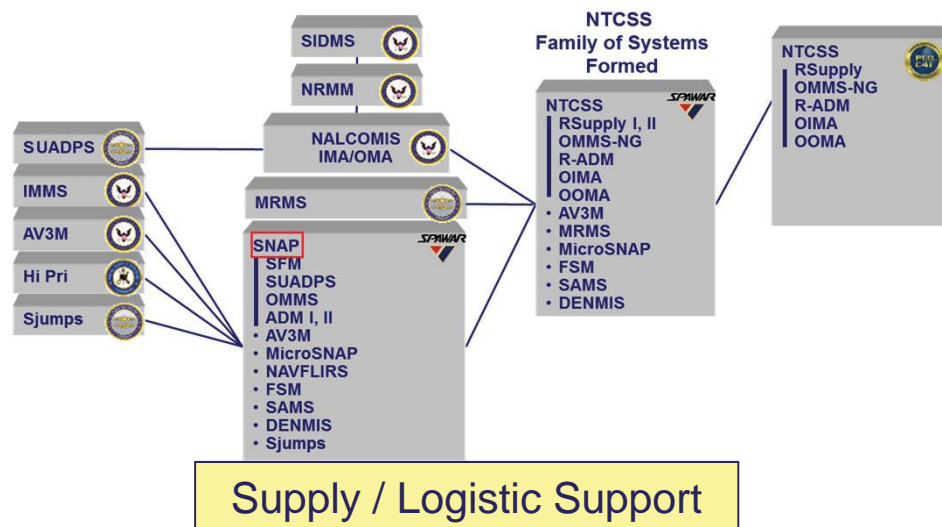
Two Examples of independent evolution and growth of single function systems

- Similar single function networks also evolved for intelligence, personnel management, training targeting, medical and many other functions

Created networks with:

- Lack of common hardware and software
- Independent training and support systems
- No common cybersecurity or information assurance tools
- Constant end of life challenges

...a real Cybersecurity Problem





First Attempts at Integrated Afloat Network



- Integrated Shipboard Network Systems (ISNS)
 - Late 1990's attempt to host or connect applications to one network
 - Internal connectivity among shipboard users
 - External internet connectivity
 - Host infrastructure to support manpower, logistics and war fighting systems
 - Connects to and provides transport to numerous systems
 - Multiple variants





The Problem

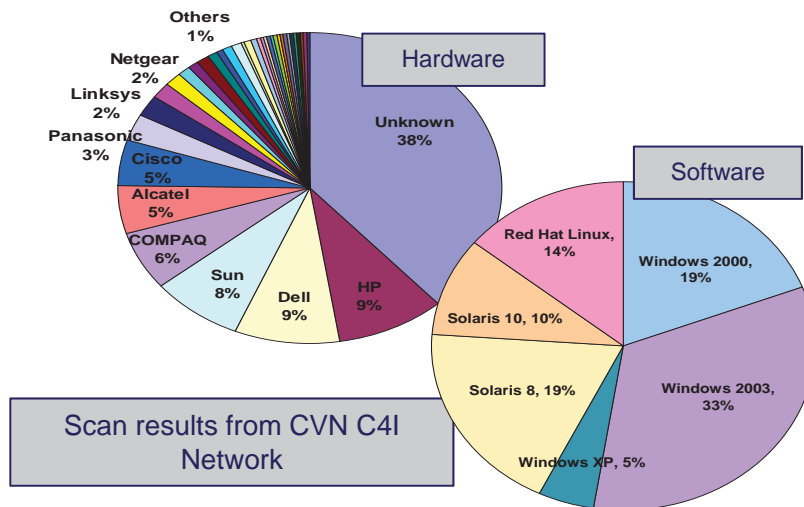
• ISNS and other legacy networks

- Over 642 different network configurations afloat
- All ISNS systems have at least one significant vulnerability
- No planned or funded hardware or software refresh

• Significant negative impacts on:

- Cybersecurity
- Interoperability
- Operational Effectiveness
- Training
- Logistics and Supportability

All ISNS Systems had at least one CAT I vulnerability – and this was before Windows XP EOL



Legacy Hardware and Software Vulnerability

Ship Class	Hardware/Software	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21
Carrier	Hardware	100%	67%	50%	25%	17%	8%	0%	0%	0%
	Software	100%	67%	50%	25%	17%	8%	0%	0%	0%
Large Deck Amphib	Hardware	100%	92%	64%	36%	18%	0%	0%	0%	0%
	Software	100%	92%	64%	36%	18%	0%	0%	0%	0%
Unit Level	Hardware	100%	82%	62%	43%	28%	18%	13%	7%	0%
	Software	100%	82%	62%	43%	28%	18%	13%	7%	0%
Submarines	Hardware	100%	98%	89%	75%	56%	34%	10%	0%	0%
	Software	100%	98%	89%	75%	58%	36%	12%	0%	0%
Orphans	Hardware	100%	100%	100%	87%	73%	56%	41%	13%	0%
	Software	100%	100%	100%	87%	73%	59%	41%	25%	0%

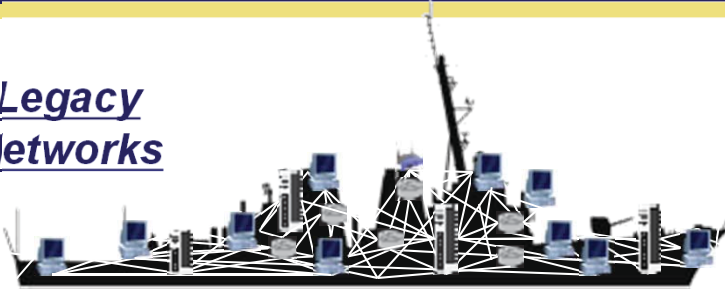
Updated Dec 2012



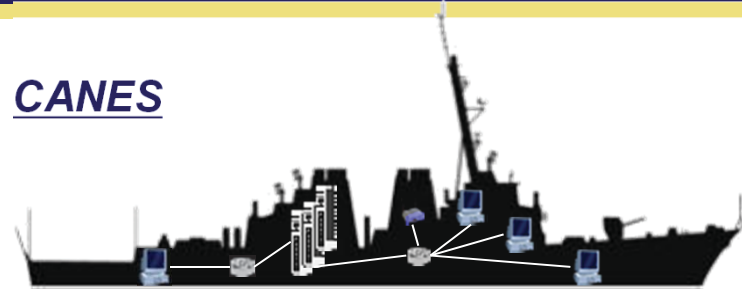
The Solution: Consolidated Afloat Network Enterprise Services (CANES)

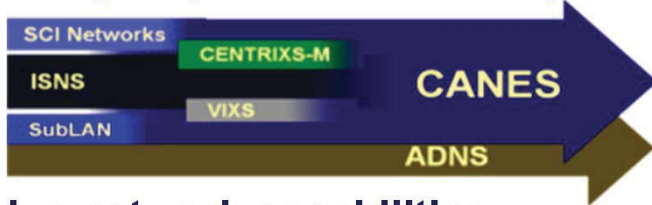


Legacy Networks



CANES



- **CANES is the Navy's Afloat IT execution strategy**
 - Transforms the network into a platform enabling significant operational capabilities
 - Replaces operationally ineffective and unaffordable networks
 - Aligns multiple programs, capabilities, requirements and resources into single PoR
- **CANES replaces five existing shipboard network systems**
- **CANES provides extensive network capabilities**
 - Data, transport, voice and video services, systems management, cybersecurity
 - Enables insertion of next generation of C2 and ISR capabilities

CANES restores afloat network agility, security, maintainability and interoperability



CANES High Level Overview

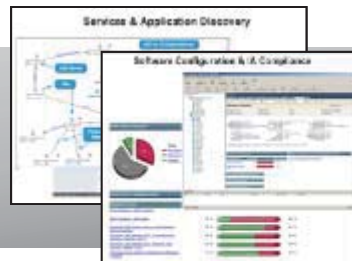
Information Assurance

Identification, Authentication & Access Control

Configuration Protected Objects

Forensics Examination Service

Systems Management



Malware Protection

Core Enterprise Services

Core Enterprise Services

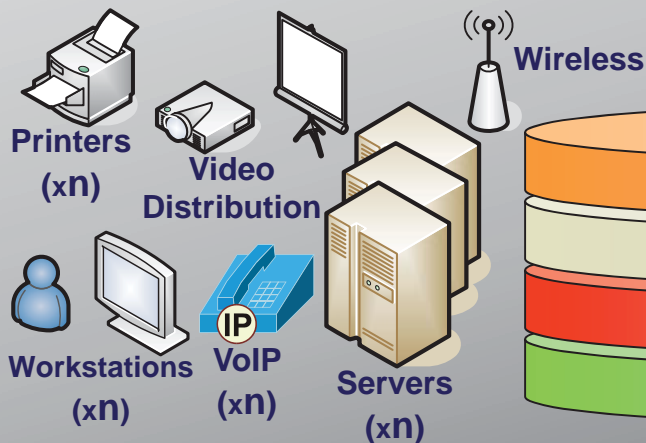
- Email/Calendar
- File Transfer
- SQL Database
- Office Productivity
- DNS
- LDAP
- PDA Synch
- Knowledge Management

Encryption Service

Computing Infrastructure

Transport

Communications



Domain 1

Domain 2

Domain 3

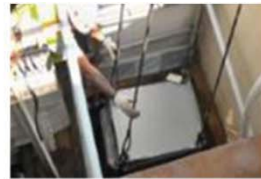
Domain 4

Boundary Protection



Afloat Cybersecurity Approach

- Certification & Accreditation Process
 - National Institute of Standards and Technology (NIST) standards
 - Regular reviews by senior certification authorities
- Patching and update notification systems and processes
 - Computer Tasking Orders, Information Assurance Bulletins
- Ship Self-Help via CANES Cybersecurity Tools
 - Industry standards and COTS tools
- Continuum of cybersecurity testing
 - From development through network and application lifecycle





Technology Approach

- **Afloat IT Opportunities / Challenges**
 - 2yr/4yr Development Refresh Cycle
 - 4yr/8yr Minor/Major Deployment Cycle
 - EOL / EOS issues – need new ideas and approaches
- **Afloat Network basics**
 - Modular design
 - Enables identification of multiple sources of supply and/or repair
 - Supports flexible business strategies to enhance competition
 - Open standards and interfaces
 - Functional partitioning facilitates replacement of individual subsystems or components and encourages multiple vendor participation

Industry partnership is key to maintaining multiple sources and driving competition



Participation and Partnership



- **PEO C4I Gaps Document**

- http://www.public.navy.mil/spawar/PEOC4I/Documents/PEOC4I_ST_Acq_GapsJune2014S.pdf
- Proposals require program endorsement for transition

PMW 160 Cybersecurity Needs

- Getting and Staying Ahead of End of Life and End of Support Cycles
- Form, Fit, Function Replacements of EOL HW (within Space Weight and Power – SWAP - constraints)
- Cybersecurity tools built into “friendly” system management and administration functions
- Threat prediction and recognition
- Supply Chain Risk Management Processes - device integrity checks, verification that we have purchased from approved vendors, etc.



Naval Enterprise Networks Cyber Security Overview

CAPT Mike Abreu, Program Manager
Program Manager, Naval Enterprise Networks Program Office
(PMW-205)
October 27, 2014

Statement A: Approved for public release, distribution is unlimited (23 OCTOBER 2014)



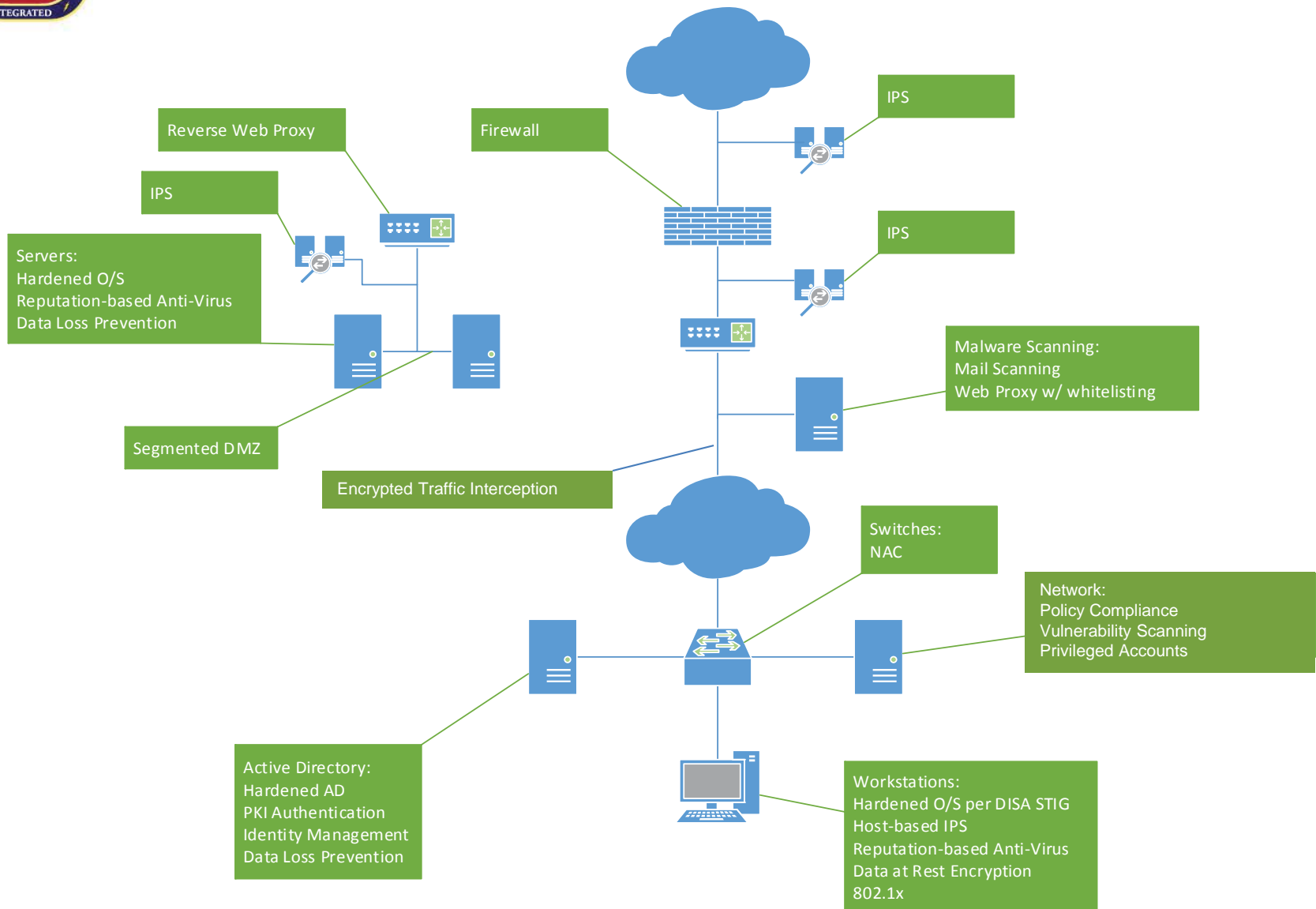
NGEN Overview

- **Transition to the NGEN Contract was completed 01 October 2014.**
- **NGEN** is a network management and services contract with HP, Inc. which:
 - Provides **secure**, net-centric data and services to United States Navy (USN) and United States Marine Corps (USMC) personnel for the NMCI network.
 - Forms the foundation for Naval Networking Environment (NNE) vision and strategy.
 - Operational in DoN CONUS facilities, plus Hawaii, Alaska and Okinawa.
- **NMCI / NGEN is the DoD's largest centrally-managed enterprise network**
 - 300,000+ seats and 700,000+ users in more than 2500 locations from major bases to individual personnel, such as recruiters, in remote sites.
 - Processes 20TB+ of web traffic data daily and 33 million+ email messages weekly
 - Blocks more than 35 million spam messages monthly
 - Maintains >99% intranet and server availability
- **NGEN will continue the migration of legacy networks, where approved and funded**
- **The program is continuing a large-scale security improvement program in cooperation with the operational authority and resource sponsor**

Industry innovation in large scale cyber defense products and techniques are critical to our ability to pace the threat

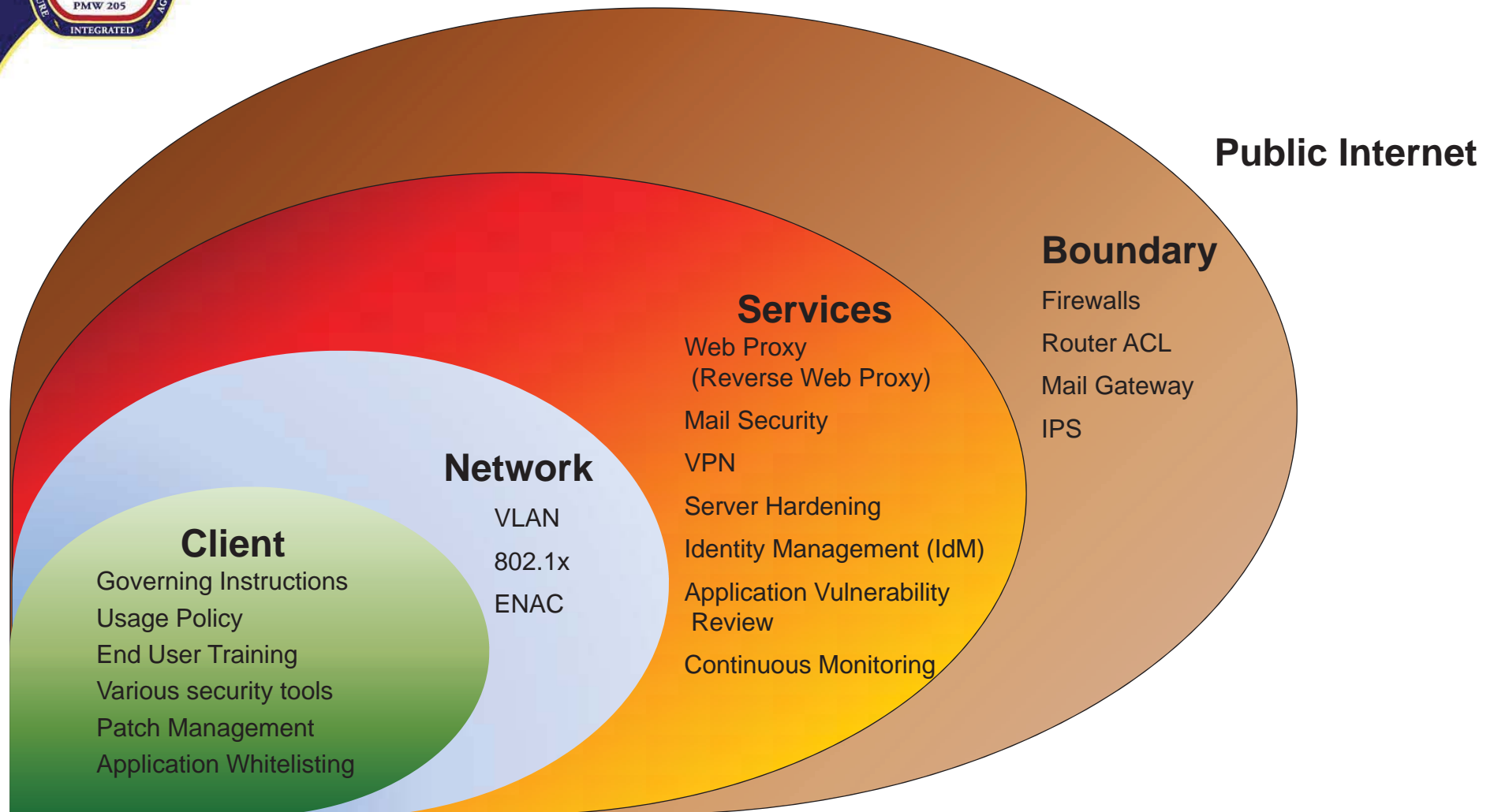


Security Environment





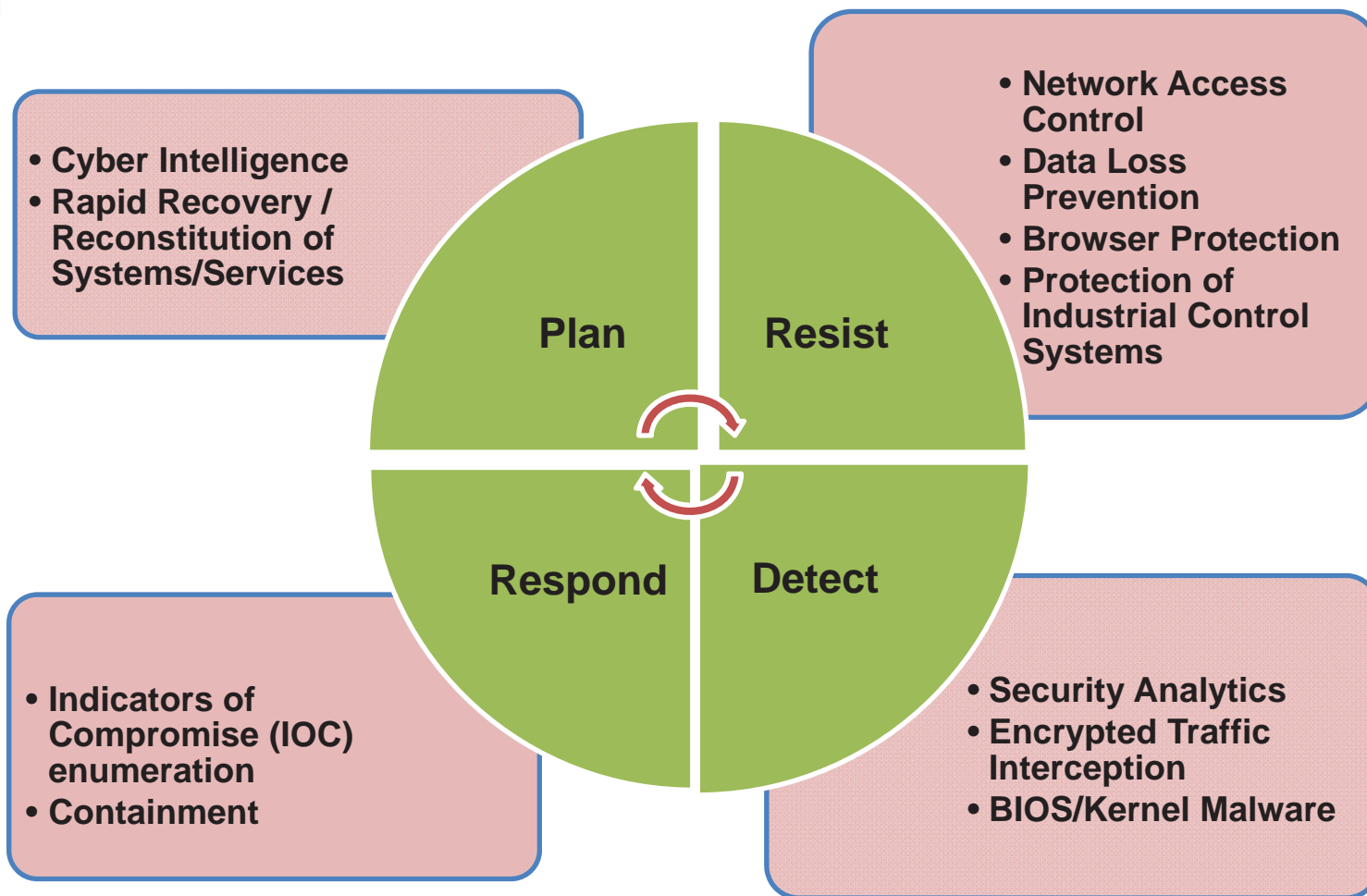
Defense in Depth



Navy and DoD implement a layered defense strategy to protect our networks and the information carried on them – industry products are key to that effective defense



Areas of Innovation Interest



We are continually assessing cyber defense improvements with our operational and resource sponsor partners and will pursue them with our prime service provider as they are approved and funded



Summary

- **Our networks are targets**
- **We are challenged to keep pace with the threat**
- **Industry products and techniques form the basis of our defense capabilities**
- **We need your help to continue to protect our networks and data in a manner that meets the warfighter mission need**



CYBER CENTER OF EXCELLENCE: STRENGTHENING CRITICAL INFRASTRUCTURE

27 October 2014

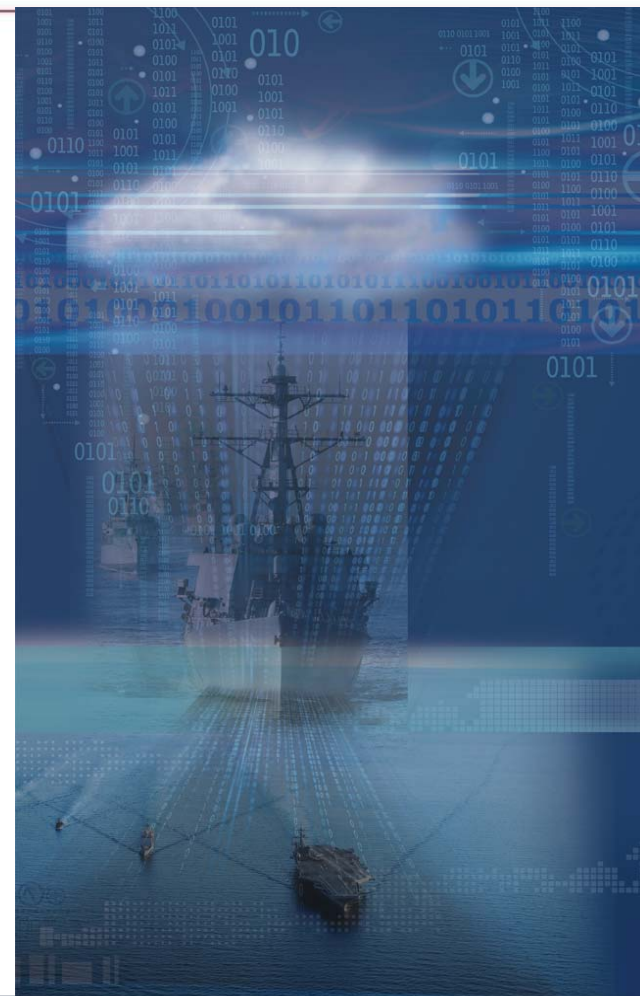


Dr. Stephen Russell

SPAWAR 7.0 Director, Science & Technology;
Chief Technology Officer

*“Our intent is to make data security and authentication a given; constant, seamless and transparent to the Navy warfighter.”**

***2014 U.S. Navy Information Dominance Science and Technology Objectives**



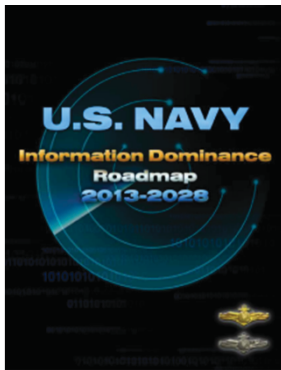


Agenda

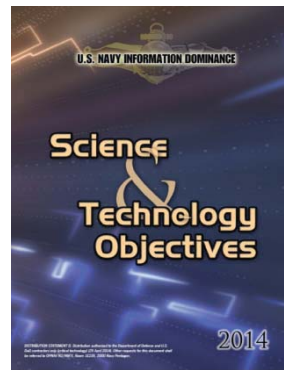
- ▼ Information Dominance (ID) S&T
 - ID S&T Products
 - Information Security and Information Assurance (ISA) S&T Focus Areas
 - Extracts from PMW 130's S&T Gaps
- ▼ SPAWAR Systems Center Thrust Areas: Cyber Security
- ▼ CYBER Initiatives
- ▼ Takeaways



Information Dominance (ID) S&T Products



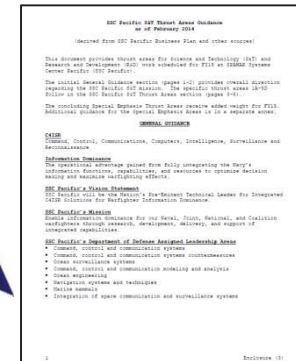
OPNAV N2/N6 -
ID Roadmap



USN ID S&T
Objectives (STOs)



PEO C4I / PMW
130 S&T
Acquisition Gaps



SSC S&T
Thrust Areas –
Cyber Annex

ID Guidance derives strategic objectives to deliver capabilities to protect Navy Networks in cyberspace and prevent compromise of C4I systems



Information Security and Information Assurance (ISA) S&T Focus Area

- ▼ Focus Area Description: The Navy is heavily reliant on the operational employment of networked Information Technologies (IT). These technologies, while powerful, are growing increasingly vulnerable.
- ▼ Technology investments in this area focus on finding innovative and cost-effective ways to mitigate those vulnerabilities through such measures



ISA S&T Focus Area (cont)

- ▼ ID-ISA-STO-01: Assured Access and Transparent Identification and Authentication across the Network
 - Develop/leverage technologies that convey seamless, transparent and comprehensive identity assurance and data authentication.
 - **PMW 130 Scope:** This includes (1) defining a universal set of user attributes and access-based policy schema and (2) a mechanism to tag data assets with such attributes and policies.
- ▼ ID-ISA-STO-02: Nimble and Proactive Network Defense Posture against Advanced Persistent Threats
 - Develop/leverage technologies that detect and eradicate advanced persistent threats, well-organized and heavily-resourced cyber-attacks that access and exfiltrate information from Navy systems.
 - **PMW 130 Scope:** Such defenses should withstand such threats as: (1) polymorphism, (2) stealth, (3) regeneration and (4) disabling of anti-malware defenses.



ISA S&T Focus Area (cont)

- ▼ ID-ISA-STO-03: Detection, Prevention and Reporting of Data Exfiltration to Counter the Insider Threat
 - Develop/leverage technologies that provide full inspection of encrypted traffic, embedded data, and compressed files—all forms for which exfiltrated data may be in to bypass detection by currently deployed data loss prevention (DLP) solutions.
 - ***PMW 130 Scope:*** Future initiatives should strengthen existing DLP solutions that accommodates the above features and identify such critical information that is to be DLP-enforced (i.e. using metadata).
- ▼ ID-ISA-STO-04: Resiliency Under Cyber Attack
 - Develop/leverage technologies and/or mechanisms which provide continued mission operations in the event of a disruptive cyber-attack and return to normal mission operations once the attack has been addressed/resolved.
 - ***PMW 130 Scope:*** Resiliency technologies and/or mechanisms should identify critical mission-supported data assets and implement continuous controls that sustain them in the event of an attack.



ISA S&T Focus Area (cont)

- ▼ ID-ISA-STO-05: Improved Information Audit & Forensics
 - Develop/leverage technologies that improve current audit capabilities for increased forensics effectiveness.
 - *PMW 130 Scope*: This includes (1) expanded information gathering down to the user level, (2) protection of audits from modification, (3) synchronization of audits across all network operations centers (NOCs), and (4) providing a backup audit capability in the event of a failure.
- ▼ ID-ISA-STO-06: Cloud Computing Security & Assurance
 - Develop technologies for cloud security to address data Confidentiality, Integrity, and Availability (CIA).



PEO C4I/PMW 130 Cybersecurity S&T Gaps

- ▼ In addition to the aligned ISA Technology Objectives, PEO C4I/PMW 130 has articulated the following cybersecurity S&T gaps:
 - Provide predictive computer network defense (CND) techniques, which utilize short-term observations and knowledge of the adversary to discover anomalies or anticipate cyber attacks that would normally not be quickly identified via proactive measures.
 - Provide a robust means of retrieving, correlating and analyzing existing and applicable defensive cyber operational data used for cyber situational awareness.



SPAWAR Systems Center Thrust Area: Cyber Security

SSC Pacific

Software assurance
Identity and Access Management
Computer network defense
Sustainable IA technologies
Cyber Situational Awareness
Cloud security
Total ownership cost - reductions for cyber security
Cryptographic devices to support Over-the-Network-Keying technologies
Key distribution and production, beyond the Key Management Infrastructure (quantum cryptography)
Secure Industrial Control Systems



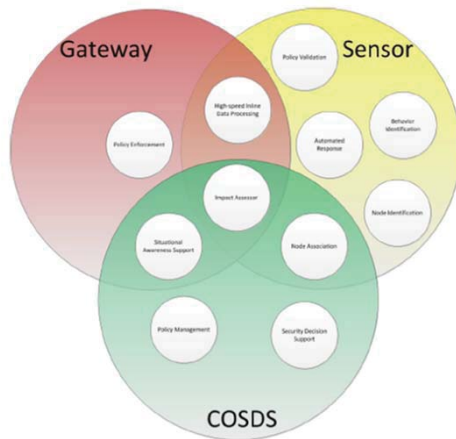
SSC Atlantic

Efficient and Resilient Routing Algorithms
Self-organization and auto configuration
Dynamic load distribution
Attack Tolerance and Detection
Data priority and context awareness
In memory computing
Novel data compression techniques
Data forensics
Data storage Data Link development
IA and Data security on distributed systems
Intelligent management and distributed processing

Protect against Advanced Persistent Threats posed by state and non-state actors with the capability and intent to relentlessly probe and attack our networks



CYBER Initiatives



Proactive Computer Network Defense/Information Assurance (CND/IA)

Intended to develop an integrated Naval CND/IA prototype/system that aids the warfighter in identifying and mitigating real-time threats while at the same time ensuring continuity of essential operations and access to assured data during attacks.

Fortifying Data with Functional/Attribute-Based Encryption

Fuses both access-based policy (developed from a series of user attributes) enforcement and encryption. Encryption of data is cryptographically embedded with an access-based policy, which ensures only the intended recipient (with an appropriate need-to-know) is able to decrypt the data.



Program Warfare Office 130



CYBER Initiatives (cont)

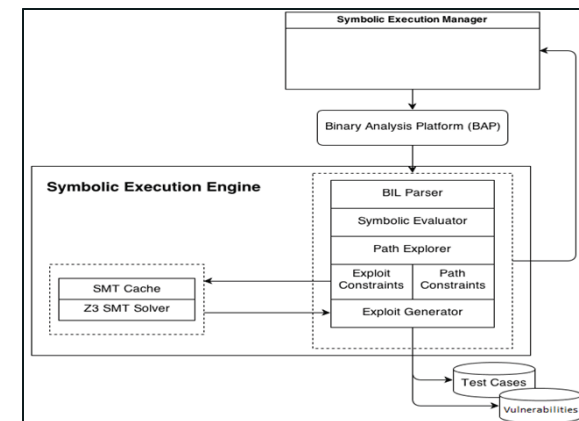


Defensive Anti-Reconnaissance Engine

Even with properly configured firewalls, attackers can still penetrate a network and launch scans from the inside. Host-based firewalls and IDS's can detect and stop scans, but they can reveal too much information to the attacker. DARE will defend against automated reconnaissance scans by intercepting and spoofing the responses to the attacker. By preventing these scans from revealing information about the network, the attacker must contend with an increased attack surface, and a larger attack footprint that increases the probability of being detected

Symbolic Execution on BIL to Discover Vulnerabilities in Binary Targets

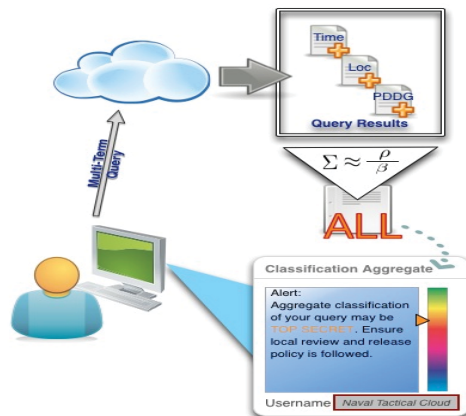
Brand new developments in binary analysis provide detailed instruction representation of a target binary. Proven software verification techniques can be used for better program analysis, and a formal definition can be created that finds and demonstrates vulnerabilities in targets due to these analysis techniques. This effort develops a formal verification system to identify vulnerabilities in binary targets. To accomplish this, custom symbolic execution engine for the BAP Intermediate Language (BIL) were developed. By combining the features of a symbolic execution engine with an SMT solver, complete and detailed conditions can be provided that identify vulnerabilities in binary programs.



SSC Atlantic



CYBER Initiatives (cont)



Aggregation of Classified Data in a Cloud Environment

Assist in the determination of aggregate classification of data queried from a cloud environment and displayed to intelligence analysts in order to provide an indication of possible escalation of classification of the finished results when compared to the discrete, queried sources.

Defend and Jump (D&J)

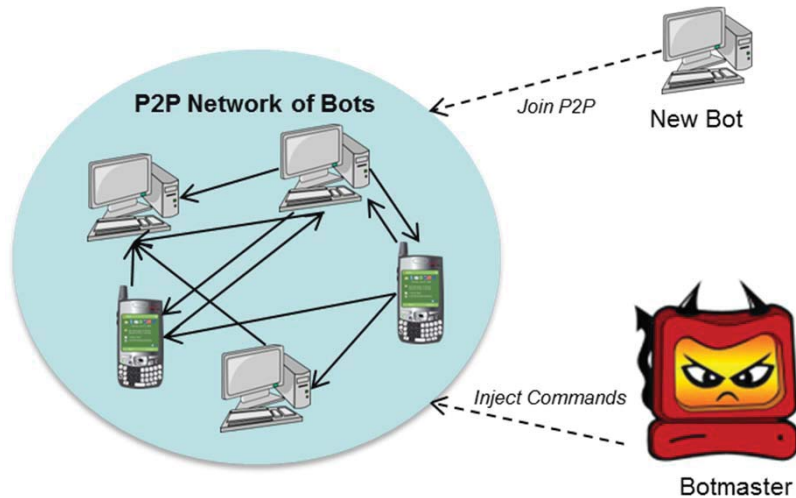
D&J proposes to improve DoD network security by introducing a capacity for dynamism: attacks that exploit the network's current state will not be sufficient to defeat an adaptive network. D&J will identify technologies that facilitate response to Computer Network Attack (CNA) and Computer Network Exploitation (CNE) through the application of Mobile Ad Hoc Wireless Networking (MANET) technology along with military wireless techniques. These measures are expected to make DoD networks increasingly resistant to state of the art attacks



SSC Atlantic



CYBER Initiatives (cont)



SILKWEB

Solution provides a means to identify compromised nodes in large networks and contributes to identifying the source of malicious activity. Constructs a "fingerprint" of known BOTNETs and generates the probability of a computer being infected.

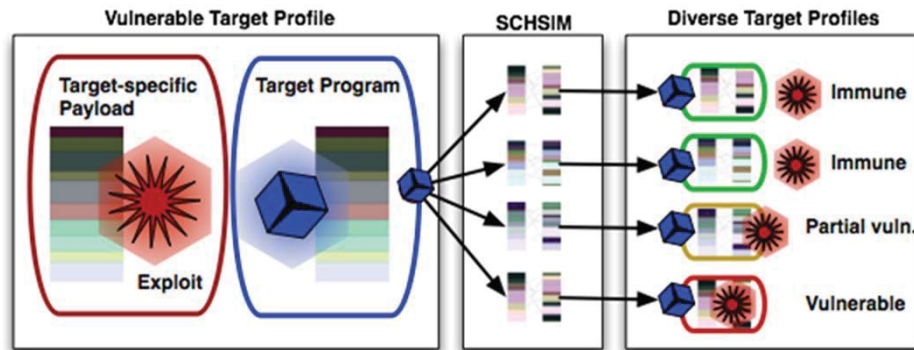
PXE Assurance Scanning System (PASS)

A networked based malware/rootkit scanning system that has the capability to scan "off-line" clients for higher malware scanning integrity and higher detection rates.



SSC Pacific

CYBER Initiatives (cont)



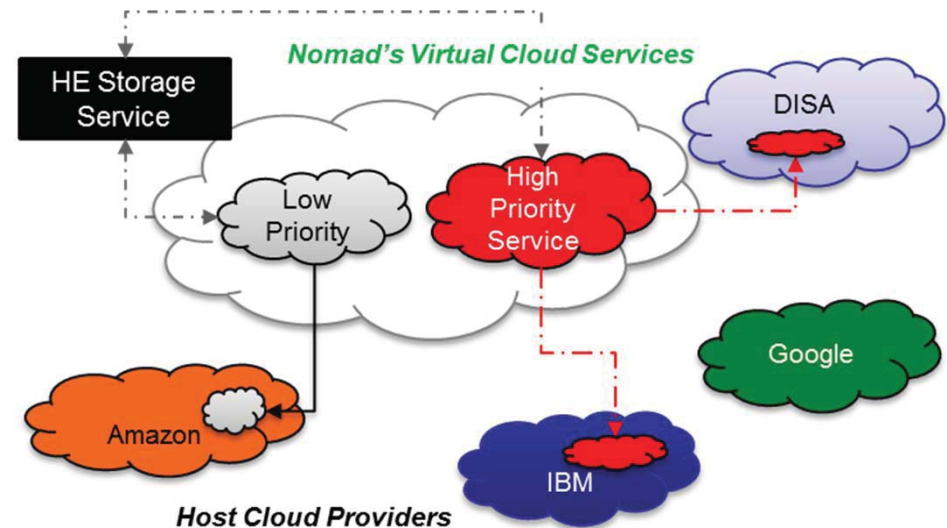
SCHSIM

Dramatically improves the security of existing information systems by improving binary diversity. This approach makes it more difficult for attackers to know latent instruction offsets, preventing code re-use attacks.

NOMAD

A high-assurance cloud service based on adaptive service migration and homomorphic encryption.

- Monitoring of cloud health status (QoS)
- Dynamic migration of compute resources across clouds
- Optimized homomorphic encryption-based storage services



SSC Pacific



Takeaways

- ▼ The Navy's Task Force Cyber Awakening is directing significant improvements to the Navy's current IA architecture.
- ▼ Navy S&T Cyber investments seek to stay ahead of our adversaries and integrate seamlessly with the Joint community.
- ▼ However, the number of S&T gaps continues to far exceed the amount of available DoD funding.
- ▼ Insight into Industry investments and partnerships with both Industry and Academia are critical for guiding and augmenting DoD efforts.





Agenda

1300 Pat Sullivan, Executive Director, SPAWAR

Overview

1330 Greg Hansford, SPAWAR Budget Officer, SPAWAR

CYBER Budget Outlook: Federal to SPAWAR

1400 Brian Marsh, Office of SPAWAR Chief Engineer

CYBER Security & Technical Authority

1430 Steve Bulard, Program Manager PMW 130

Information Assurance & Cyber Security

1500 CAPT Ben McNeal, Program Manager PMW 160

Afloat Tactical Networks Cyber Security

1530 CAPT Michael Abreu, Program Manager PMW 205

Ashore Naval Enterprise Networks Cyber Security

1600 Dr. Stephen Russell, Director, Science and Technology, SPAWAR

Cyber Security Science & Technology

QUESTIONS